PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 121/4

A2

(11) International Publication Number: WO 99/19822

(43) International Publication Date: 22 April 1999 (22.04.99)

(21) International Application Number: PCT/US98/19352

(22) International Filing Date: 16 September 1998 (16.09.98)

(30) Priority Data:
08/949,438 14 October 1997 (14.10.97) US

(71) Applicant: MICROSOFT CORPORATION [US/US]; One Microsoft Way, Redmond, WA 98052-6399 (US).

(72) Inventors: BIRDWELL, Kenneth, J.; 17452 N.E. 12th Street, Bellevue, WA 98008-3816 (US). YACOBI, Yacov; 5050 W. Mercer Way, Mercer Island, WA 98040 (US).

(74) Agents: LEE, Lewis, C. et al.; Suite 430, W. 201 North River Drive, Spokane, WA 99201 (US).

(81) Designated States: JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: SYSTEM AND METHOD FOR DISCOVERING COMPROMISED SECURITY DEVICES

(57) Abstract

A data delivery system has a content server or other mechanism for delivering encoded content to multiple authorized clients. The authorized clients are equipped with security devices having decoding capabilities to decode the content. Unauthorized clients are prevented from decoding the content because they are not supplied with the decoding capabilities. As part of the data delivery system, a traitor detection system is provided to discover an identity of an authorized client that has been compromised and is illicitly transferring decoding capabilities to unauthorized clients. The traitor detection system generates different decoding capabilities and creates an association file which relates the different decoding capabilities to different authorized clients. The decoding capabilities are traced to determine which of them is illicitly transferred to an illegitimate user. In the event that one of the decoding capabilities is illicitly transferred, the traitor detection system consults the association file to identify one or more of the authorized clients that were originally supplied with the illicitly transferred decoding capabilities. The identified set of clients includes the compromised client. The process is repeated for the identified set of clients with a new set of decoding capabilities to successively narrow the field of possible pirating clients, until the compromised security device is precisely pinpointed.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SYSTEM AND METHOD FOR DISCOVERING COMPROMISED SECURITY DEVICES

TECHNICAL FIELD

This invention relates to a data delivery system in which data is encrypted and served to multiple clients that are authorized to decrypt the data. More particularly, this invention relates to systems and methods for discovering authorized clients that have been compromised and are illicitly transferring decryption capabilities to unauthorized clients so that the unauthorized clients can decrypt the data.

BACKGROUND OF THE INVENTION

It is common in the digital age to deliver data in an encoded format to prevent unauthorized eavesdroppers from gaining access to the data. Conventional bi-directional communication between two parties protects data transmissions using well-established protocols and cryptographic techniques. The sender encrypts the data in a manner that only the receiver can decrypt and verify as being sent from the sender.

A slightly more difficult problem concerns the broadcast or multicast delivery of data over a unidirectional network from one source to many receivers. Well-known systems of this type include broadcast and cable television, radio, satellite entertainment, and network multicasting. There are different techniques for protecting the data during delivery. One common technique used in cable and satellite television is to scramble the data prior to transmission. Authorized users are equipped with cable decoders or satellite descramblers to descramble the data after transmission. The descramblers are usually implemented as hardware devices having a decoding chip or software code for decrambling the data transmission. Unauthorized users who intercept the data transmission are prevented from decoding the data because they do not possess the descrambler.

Cryptographic solutions can also be used to protect broadcast data delivery. The data is encrypted at the content provider prior to transmission and broadcast in the encrypted format. Authorized users are given keying materials before or during the broadcast for use in decrypting the data. Unauthorized users can eavesdrop on the data transmissions, but are unable to decrypt the data into meaningful information without access to the keying materials. As a result, the data transmissions are secure.

In such data delivery mechanisms, the decoding capabilities are implemented in hardware- or software-based security devices located at the authorized users' residents. Due to this isolation, the security devices are susceptible to being compromised. Despite the best devised plans, protection schemes will inevitably be attacked by pirates who attempt to circumvent the protection schemes for purposes of illegal gain. With sufficient time and resources, a pirate masquerading as an authorized user can patiently reverse engineer a descrambling code or deduce cryptographic keying material. Once the security device is compromised, the pirate can illicitly sell the decoding information to unauthorized users for illegal profit, allowing the unauthorized users to receive the data transmission.

This inventors have developed a system and method which addresses the problems of pirate attacks.

SUMMARY OF THE INVENTION

This invention concerns a system and method for tracing distribution of decoding information to authorized clients in an effort to discover any authorized clients that have been compromised and are illicitly transferring the decoding information to unauthorized clients.

According to one aspect of this invention, a data delivery system has a content server or other mechanism for delivering encoded content to multiple authorized clients. In one implementation, the content is encrypted using a cryptographic keying material,

although other encoding protocols may be used. The authorized clients are equipped with security devices having decoding capabilities, such as decryption keying materials, to decode the content. Unauthorized clients are prevented from decoding the content because they are not supplied with the decoding capabilities.

As part of the data delivery system, a traitor detection system is provided to discover an identity of an authorized client that has been compromised and is illicitly transferring decoding capabilities to unauthorized clients. The traitor detection system generates different decoding capabilities and creates an association file which relates the decoding capabilities to different authorized clients. The decoding capabilities are traced to determine which of them is illicitly transferred to an illegitimate user. In the event that one of the decoding capabilities is illicitly transferred, the traitor detection system consults the association file to identify one or more of the authorized clients that were supplied with the illicitly transferred decoding capabilities as a possible source of the illicit transfer. The process is repeated for the identified clients with a new set of decoding capabilities to successively narrow the field of possible pirating clients, until the compromised security device is identified.

The number of decoding capabilities for each detection cycle can be varied from two at the low end, to one-per-client at the high end. With two-per-cycle, the population of clients is successively reduced by half with detection occurring at log base two of the number of clients. This approach requires more detection cycles to identify the compromised security device, but involves less generation and distribution of decoding capabilities for each cycle. At one-per-client, the compromised security device can be found in one detection cycle, but at a tradeoff in that the amount of decoding capabilities sent along with the data transmission is quite large.

In another implementation, the data transmission is segmented into M blocks. For each transmission block, the traitor detection system supplies N different keys to N groups of authorized security devices. The keys enable the security devices to receive

that block of the data transmission. When a key is found to be illicitly transferred, the traitor detection system identifies the group of authorized security devices that was sent that key. For the next block, the traitor detection system supplies a new set of N different keys to N groups of security devices within the previously identified group. This process is repeated for each block of the transmission. Proper selection of parameters M and N results in identification of the compromised security device by the end of the transmission. For example, for 10,000 authorized clients, a data transmission can be segmented into four blocks (i.e., M=4), with each block having 10 different keys (i.e., N=10) being supplied for each detection cycle.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a diagrammatic illustration of a data delivery system for sending data over a network to multiple authorized clients according to one implementation. Fig. 1 also shows an illicit transfer of decoding capabilities from an authorized client to an unauthorized client.

Fig. 2 is a block diagram of a server computing unit.

Fig. 3 is a block diagram of an authorized client computing unit.

Fig. 4 is a block diagram of a cryptographic unit resident at the client.

Fig. 5 is a flow diagram showing steps in one method for discovering an identity of an authorized client that is illicitly transferring authorization keys to unauthorized clients.

Fig. 6 is a flow diagram showing steps in another method for discovering an identity of a compromised client.

Fig. 7 is a diagrammatic illustration of a data transmission delivered according to the Fig. 6 method.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

This invention concerns techniques for discovering an identity of authorized clients that have been compromised and are illicitly transferring decoding capabilities to unauthorized clients. For purposes of discussion, the decoding capabilities are described in a preferred implementation of cryptographic technologies having keying materials for encryption and decryption of data. The following discussion assumes that the reader is familiar with cryptography. For a basic introduction to cryptography, the reader is directed to a text written by Bruce Schneier and entitled, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," published by John Wiley & Sons, copyright 1994 (second edition 1996), which is hereby incorporated by reference.

In the following description, the invention is described in the context of an exemplary system architecture for delivery of content to broadcast-enabled personal computers (PCs). In this architecture, data can be served from multiple servers concurrently over a data network, such as the Internet, to a broadcast station where it is transmitted over a broadcast network to the broadcast-enabled PCs. However, the invention may be implemented in other system architectures. For instance, the invention can be implemented in the context of conventional cable or RF television distribution architecture in which content is broadcast from a station to multiple televisions. As another alternative, the invention can be implemented in a conventional network architecture in which content is sent from a server to multiple clients using, for example, a multicast protocol.

Fig. 1 shows an exemplary data delivery system 20 in which content is delivered from multiple content servers 22(1), 22(2), ..., 22(K) to multiple clients 24(1), 24(2), 24(3), ..., 24(M). In this implementation, the content servers 22(1)-22(K) are connected to a broadcast center 26 via a bi-directional data network 28 which enables two-way communication between the content servers 22(1)-22(K) and the broadcast center 26. The content servers serve content in the form of audio, video, animation, bit maps or

other graphics, applications or other executable code, text, hypermedia, or other types of data.

The bi-directional data network 28 represents various types of networks, including the Internet, a LAN (local area network), a WAN (wide area network), and the like. The data network 28 can be implemented in a number of ways, including wire-based technologies (e.g., fiber optic, cable, wire, etc.) and wireless technologies configured for two-way communication (e.g., satellite, RF, etc.). The data network 28 can further be implemented using various available switching technologies (e.g., ATM (Asynchronous Transfer Mode), Ethernet, etc.) and different data communication protocols (e.g., TCP/IP, IPX, etc.).

The broadcast center 26 receives the data served from the content servers 22(1)-22(K) over the network 28 and broadcasts the data over a broadcast network 30 to the clients 24(1)-24(M). The broadcast network 30 can be implemented in a variety of ways, including satellite, radio, microwave, cable, and the like.

The broadcast center 26 includes a router 32, a signal generator 34, and a broadcast transmitter 36. The router 32 is coupled to the bi-directional data network 28 to receive the data served over the network 28 from the content servers 22(1)-22(K). The router 32 is a final node of the data network 28 in which data communication is bi-directional to that point and unidirectional past that point. The router 32 is preferably configured as a bridge-router between the traditional data network 28 and the broadcast network 30. A bridge-router is capable of supporting video and audio broadcast transmission. The router 32 converts the data from a network packet format to a format appropriate for broadcast transmission. The signal generator 34 generates a broadcast signal with the data embedded thereon to carry the data over the broadcast network 30. The broadcast signal is passed to the transmitter 36 where it is broadcast over the broadcast network 30 to the clients 24(1)-24(M). The clients might still be able to communicate with the broadcast center 26 or content servers 22(1)-22(K) using a

different back channel, such as a connection to the data network 28, but this aspect is not shown in the drawings.

The data is encrypted at the content servers 22(1)-22(K) prior to transmission to ensure secure delivery over the data network 28 and broadcast network 30. As an alternative, the data can be encrypted at the broadcast center 26 prior to broadcast transmission. Authorized clients 24(1)-24(K) are provided with decryption capabilities, represented by a key 38, to decrypt the data. The decryption capabilities are described below in more detail with reference to Fig. 3. The clients 24(1)-24(M) can be implemented in a number of ways, including desktop computers, laptop computers, televisions with set-top boxes, and computer enhanced television units. In this exemplary implementation, the clients are broadcast-enabled PCs which are described below in more detail with reference to Fig. 3.

An unauthorized client 39 is also shown in Fig. 1. The unauthorized client 39 can be similar to an authorized client in every respect, except that the unauthorized client is not legitimately equipped with the decryption capabilities. Instead, the unauthorized client 39 obtains the decryption capabilities through illegal transfer from one of the authorized clients 24(1)-24(M).

For this discussion, assume that the last authorized client 24(M) has been compromised. An otherwise legitimate user who has decided to engage in illegal pirating conduct has broken the cryptographic cipher in the client's security device and is capable of obtaining the keying material for upcoming data transmissions. The pirate sells the keying material on a black market to enable unauthorized clients, such as unauthorized client 39 to receive and decipher the content. This is illustrated by the dashed line showing an illicit transfer of the key 38 from the authorized client 24(M) to the unauthorized client 39.

Fig. 2 shows an exemplary implementation of a content server 22(1) that is configured to both serve the content in an encrypted format and to supply the keying

material. In this implementation, the content server 22(1) generates the keying materials used to encrypt the content and transmits the keying materials ahead of the content to the authorized clients 24(1)-24(M). In other implementations, different servers might be employed to separate the functions of key generation and management and content serving. Additionally, the keying materials might be supplied in other ways besides transmission over the networks. For instance, authorization keys which permit access to the data transmission stream might be supplied routinely (e.g., once a week) on a disk to the authorized users.

In Fig. 2, the content server 22(1) includes a server computer 40 having a processor 42 (e.g., Pentium® Pro microprocessor from Intel Corporation), volatile memory 44 (e.g., RAM), and program memory 46 (e.g., ROM, flash, disk drive, floppy disk drive, CD-ROM, etc.). The computer 40 is configured, for example, as a personal computer or workstation running a multitasking, disk-based operating system, such as Windows® NT from Microsoft Corporation. The server computer 40 is connected to the data network 28 via a network connection 48. The content server 22(1) has multiple storage disks 50 which are implemented as a disk array to store various forms of content. In this illustration, the content server 22(1) is shown configured as continuous media file server which serves video and audio data files from a disk array of storage disks 50. However, the content server 22(1) may also be configured to serve other forms of data.

The server 22(1) is illustrated with two software programs: a key generator 52 and a key/client associator 54. Each program is stored in program memory 46, loaded into volatile memory 44 when launched, and executed on the processor 42. The key generator 52 produces cryptographic keys that are used to encrypt the data served by the server 22(1) and to decrypt the data when it reaches the clients. More particularly, the key generator 52 creates two tiers of random symmetric keys. The keys in the first tier are called "session keys" and are used to encrypt the data being served. The session keys are given out just before the data transmission. The keys in the second tier are referred to as

"authorization keys" and are used to encrypt the session keys. The authorization keys are distributed to authorized clients well ahead of the data transmission.

In a "symmetric" cipher, the encryption key can be calculated from the decryption key, and vice versa. In many cases, the encryption key and the decryption key are the same. The symmetric key must be known to both the sender and receiver, but otherwise kept secret. Once the symmetric key is divulged, any party can encrypt or decrypt messages. Examples of suitable symmetric ciphers include DES (Data Encryption Standard) with triple-DES keys, IDEA, RC4, Diffie-Hellman, and the like.

Accordingly, prior to transmission, the data is encrypted by a symmetric encryption algorithm "E" using the session key "Ksession" as follows:

$$E_{Ksession}\,(Data) = Encrypted\ Data$$

The session key "Ksession" is then encrypted by a symmetric encryption algorithm "E" using the authorization key "Kauthorization" as follows:

$$E_{Kauthorization}\,(Ksession) = Encrypted\ Session\ Key$$

The authorization keys are preferably distributed to the authorized clients 24 in encrypted format using the authorized clients' public keys of asymmetric key pairs. An "asymmetric" key algorithm involves two separate keys, a public key and a private key. The keys are based upon a mathematical relationship in which one key cannot be calculated (at least in any reasonable amount of time) from the other key. The public key is distributed to other parties and the private key is maintained in confidence by the holder. The asymmetric public and private keys ensure two results. First, only the holder of the private key can decrypt a message that is encrypted with the corresponding public key. Second, if another party decrypts a message using the public key, that party can be

assured that the message was encrypted by the private key and thus originated with someone (and presumably the holder) of the private key. An example asymmetric cipher is the well-known RSA cryptographic algorithm named for the creators Rivest, Shamir, and Adleman.

To distribute an authorization key to an authorized client 24(1), for example, the server encrypts the authorization key in an asymmetric encryption algorithm "E" using the public key of the authorized client 24(1) "Kpub_24(1), as follows:

$$E_{Kpub\_24(1)}(Kauthorization) = \text{Encrypted Authorization Key}$$

Authorized clients are equipped with the decryption capabilities necessary to decrypt the symmetric keys and data. In this example, the authorized clients possess decryption units that can decrypt the authorization key, and then decrypt the session key and the data.

Fig. 3 shows an exemplary configuration of an authorized client 24(1) implemented as a broadcast-enabled computer. It includes a central processing unit 60 having a processor 62 (e.g., x86 or Pentium® microprocessor from Intel Corporation), volatile memory 64 (e.g., RAM), and program memory 66 (e.g., ROM, Flash, disk drive, floppy disk drive, CD-ROM, etc.). The client 24(1) has one or more input devices 68 (e.g., keyboard, mouse, etc.), a computer display 70 (e.g., VGA, SVGA), and a stereo I/O 72 for interfacing with a stereo system.

The client 24(1) includes a digital broadcast receiver 74 (e.g., satellite dish receiver, RF receiver, microwave receiver, multicast listener, etc.) and a tuner 76 which tunes to appropriate frequencies or addresses of the broadcast network 30 (Fig. 1). The tuner 76 is configured to receive digital broadcast data in a particularized format, such as MPEG-encoded digital video and audio data, as well as digital data in many different forms, including software programs and programming information in the form of data

files. The client 24(1) also has a modem 78 which provides dial-up access to the data network 28 to provide a back channel or direct link to the content servers 22. In other implementations of a back channel, the modem 78 might be replaced by a network card, or an RF receiver, or other type of port/receiver which provides access to the back channel.

The client 24(1) runs an operating system which supports multiple applications. The operating system is preferably a multitasking operating system which allows simultaneous execution of multiple applications. The operating system employs a graphical user interface windowing environment which presents the applications or documents in specially delineated areas of the display screen called "windows." One preferred operating system is a Windows® brand operating system sold by Microsoft Corporation, such as Windows® 95 or Windows® NT or other derivative versions of Windows®. It is noted, however, that other operating systems which provide windowing environments may be employed, such as the Macintosh operating system from Apple Computer, Inc. and the OS/2 operating system from IBM.

One example implementation of a broadcast-enabled PC is described in a co-pending U.S. Patent Application Serial No. 08/503,055, entitled "Broadcast-Enabled Personal Computer," filed January 29, 1996 in the names of Gabe L. Newell, Dan Newell, Steven J. Fluegel, David S. Byrne, Whitney McCleary, James O. Robarts, Brian K. Moran; William B. McCormick, T.K. Backman, Kenneth J. Birdwell, Joseph S. Robinson, Alonzo Gariepy, Marc W. Whitman, and Larry Brader. This application is assigned to Microsoft Corporation, and is incorporated herein by reference.

The client 24(1) is illustrated with a key listener 80 to receive the authorization and session keys transmitted from the server. The keys received by listener 80 are used by the cryptographic security services implemented at the client to enable decryption of the session keys and data. Cryptographic services are implemented through a combination of hardware and software. A secure, tamper-resistant hardware unit 82 is

provided external to the CPU 60 and two software layers 84, 86 executing on the processor 62 are used to facilitate access to the resources on the cryptographic hardware 82.

The software layers include a cryptographic application program interface (CAPI) 84 which provides functionality to any application seeking cryptographic services (e.g., encryption, decryption, signing, or verification). One or more cryptographic service providers (CSPs) 86 implement the functionality presented by the CAPI to the application. The CAPI layer 84 selects the appropriate CSP for performing the requested cryptographic function. The CSPs 86 perform various cryptographic functions such as encryption key management, encryption/decryption services, hashing routines, digital signing, and authentication tasks in conjunction with the cryptographic unit 82. A different CSP might be configured to handle specific functions, such as encryption, decryption, signing, etc., although a single CSP can be implemented to handle them all. The CSPs 86 can be implemented as dynamic linked libraries (DLLs) that are loaded on demand by the CAPI, and which can then be called by an application through the CAPI 84.

CSPs are explained in greater detail in a co-pending U.S. Patent Application, Serial Number 08/496,801, filed June 29, 1995, entitled "Cryptography System and Method for Providing Cryptographic Services for a Computer Application." This co-pending application was filed under the names of Terrence R. Spies, Jeffrey F. Spelman, and Daniel R. Simon and is assigned to Microsoft Corporation. The 08/496,801 application is incorporated herein by reference.

Fig. 4 shows the cryptographic unit 82 in more detail. It includes a logic unit 90, a secure non-volatile memory 92, and an interface 94 to the client. These components are constructed with tamper-resistant integrated circuit chips that are hardened against external scanning and are constructed using semiconductor processes that render it difficult to reverse engineer through layer-by-layer dissection. The interface 94 is

preferably a high speed interface, such as a PCI bus connection. Other high speed connections include VLB and 1394 serial connections. The connection between the cryptographic unit 82 and client CPU 60 does not need to be secure.

Internal to the cryptographic hardware 82 is a public/private key pair which is randomly generated during manufacturing. A private key 96 is confidentially maintained within the device and never exposed, while a public key 98 can be exported to the client. Each client security device has its own public/private key pair which can be used as a means for identification of the client for purposes of distributing authorization keys. The public/private key pair are shown stored in memory 92, although the private key may be hardcoded into the unit. The public key is signed by the manufacturer to produce a signature 100 which can be exported for purposes of authenticating the hardware unit. Both the public key 98 and the manufacture signature 100 can be passed to the client CPU 60.

The cryptographic unit 82 has an asymmetric key cryptographic cipher 102 which provides cryptographic functions involving the public/private key pair, such as decryption of an authorization key 104 for a data transmission. The asymmetric cipher 102 is implemented in hardware as part of the logic unit 94. A suitable asymmetric cipher is the RSA algorithm. The cryptographic unit 82 also has a high speed symmetric key cryptographic cipher 106 implemented in the logic unit 94. The symmetric cipher 104 is used to decrypt session keys 108 and the data itself. Symmetric ciphers offer suitable real-time speed for bulk decryption of data, whereas asymmetric ciphers are too slow for general bulk decryption. A suitable symmetric cipher is the Triple-DES Cipher-Block-Chaining algorithm, although other ciphers are acceptable (e.g., IDEA, RC4, etc.).

When the client 24(1) receives the authorization key that has been previously encrypted using the client's public key, the key listener 80 invokes the CAPI 84 and CSP 86 to perform the decryption of the authorization key. The authorization key is passed in its encrypted format from the CSP 86 through to the cryptographic unit 82. The

asymmetric cipher 102 uses the confidential private key 96 (i.e., "Kpri_24(1)") to decrypt the authorization key according to a decryption function "D," as follows:

$$D_{Kpri\_24(1)} \text{ (Encrypted Authorization Key)} = \text{Kauthorization}$$

The authorization key 104 is stored in secure memory 92 and subsequently used to decrypt the data. The client CPU 60 cannot read or access the authorization key 104; rather, the authorization key is maintained in confidence within the tamper-resistant hardware unit 82. Upon receipt of the encrypted session key, the symmetric cipher 106 is invoked to decrypt the session key. The symmetric cipher 106 uses the authorization key 104 to decrypt the session key as follows:

$$D_{Kauthorization} \text{ (Encrypted Session Key)} = \text{Ksession}$$

The session key 108 is likewise stored in secure memory 92. As the client receives the encrypted data, the data is directly passed to the cryptographic unit 82 in an encrypted format. The symmetric cipher 106 uses the session key 108 to decrypt the data as follows:

$$D_{Ksession} \text{ (Encrypted Data)} = \text{Data}$$

All decryption is accomplished within the hardware unit 82. The recovered data is passed back to the client CPU.

Utilizing three different levels of keys offers some advantages. By using a public key protocol to deliver the authorization keys, any server can generate keys for any client without intervention by a central authority. Because each server 22(1)-22(K) is independent and generates their own symmetric keys, the compromise of one server's

keys does not jeopardize any other server. By using authorization keys to distribute session keys, the server has tremendous flexibility to assign what session keys the client can receive. In the case of subscription services, for example, the content server can establish a set of transmissions that the client is authorized to receive, while holding out other transmissions that the client is not authorized to receive.

Under normal operating conditions, the data delivery system 20 can be configured to provide one authorization key for each data transmission (e.g., one key per television show or movie), or one authorization key for several transmissions (e.g., one key for four movies), or one authorization key for a period of time (e.g., one key per day or week). Since the private key, authorization key, and session key are kept confidential in the cryptographic unit 82 and the decryption is performed in the unit, the client CPU 60 is unable to obtain the keys and share them with others.

With sufficient resources and time, however, the cryptographic units may be compromised in a manner that permits the pirating user to transfer the authorization keys to unauthorized clients, such as client 39 in Fig. 1. When pirating activity occurs, the system operators often learn of the illegal activity. For instance, undercover law enforcement agencies or private investigators might covertly purchase authorization keys on a black market or from a broker of stolen goods. The existence of pirated keys reveals that a client has been compromised; but this knowledge does not, unfortunately, lead to identification of the specific client because many authorized clients receive the same authorization keys.

Fig. 5 shows exemplary steps in a method for discovering an identity of an authorized client that is known to be compromised as illicitly transferring authorization keys to unauthorized clients. The steps are implemented in hardware and software resident at either the content server, the authorized clients, or the unauthorized clients, as identified in the figure. The steps are described with reference to Figs. 1-4.

To trace the illicit activity, the key generator 52 in server 22(1) generates one or more session keys and multiple authorization keys for a single data transmission (step 120 in Fig. 5). The key/client associator 54 relates the different authorization keys to different authorized clients (step 122). As one example, the key/client associator 54 constructs a key/client association table 56 which inherently associates through its data structure the authorization keys and clients. The table 56 can be organized with a key data field to hold the authorization keys and a client data field to information identifying the client, such as a client ID or the client's public key.

In the simplest version, the content server 22(1) generates two authorization keys, assigning the first authorization key to one half of the clients and the second authorization key to the other half of the clients. At the opposite extreme, the content server can generate one authorization key for every client, to provide a one-to-one correspondence between the keys and clients.

At step 124 in Fig. 5, the authorization keys are distributed to the clients well ahead of any data transmission. The authorization keys are preferably encrypted using the public keys of the associated clients, although they may be delivered on a storage medium or the like directly to the appropriate authorized clients. The server encrypts the data with the one or more session keys (step 126) and then encrypts the session keys with the authorization keys (step 128). The encrypted session keys are transmitted over the networks to the authorized clients 24(1)-24(M) just before the data transmissions.

At the authorized clients, the cryptographic unit 82 uses the authorization key it was assigned to decrypt the one or more session keys (step 132 in Fig. 5). The cryptographic unit 82 then uses the session keys to decrypt the data (step 134).

Now, suppose that one authorized client illicitly transfers the authorization key to an unauthorized client, as represented by the dashed flow line from step 132 to step 136 in Fig. 5. This illicit transfer allows the unauthorized client to eavesdrop on the data

transmission, decrypt the session keys using the illicitly transferred authorization key (step 136 in Fig. 5), and to decrypt the data using the session keys (step 136).

Through surveillance techniques, the illicitly transferred authorization key is discovered. With this evidence, the server operator can trace the authorization key to the client(s) that were assigned the authorization key (step 140 in Fig. 5). The server cross-references the discovered authorization key via the key/client association file to identify the authorized client(s) that received the authorization key. Depending on the ration of keys to clients, the process either narrows the population of suspect clients, or precisely identifies the traitor client (step 142 in Fig. 5).

For example, if the clients are split into two groups, each with a different authorization key, the process will halve the population of possible traitors with each cycle. For precise identification, the process requires a number of iterations equal to log base two of the number of clients in the population. The process can be sped up by increasing the number of authorization keys given out. If ten keys are distributed for each cycle, the population of potential traitors is reduced by a factor of 10 each iteration. On the other hand, if a unique authorization key is given to each client, the traitor can be identified after only one iteration. A one-to-one distribution comes at a cost of generating and distributing a large number of keys. Accordingly, the specific implementation parameters are selected with this tradeoff in mind.

Figs. 6 and 7 show an alternative method which enables positive identification of a compromised client after a single data transmission. With this method, the data transmission is segmented into multiple blocks "i," where i = 1 to M (step 150 in Fig. 6). For the first block (i.e., i = 1) of the data transmission (step 152 in Fig. 6), the key generator 52 at the content server generates N different authorization keys (step 154). The key/client associator 54 associates the N authorization keys with N separate groups of clients (step 156 in Fig. 6).

The first set of N authorization keys are distributed to the respective groups of clients (step 158 in Fig. 6). The server also delivers the first block of the data transmission (step 160). The clients use the authorization keys to decrypt the session keys for the first block of the data transmission to enable the client to receive and decrypt the first block of data. The first N authorization keys cannot be used, however, to decrypt session keys belonging to subsequent blocks in the data transmission.

Sometime after the first authorization keys are distributed, the server operator learns that one of the N keys has been illicitly transferred from an authorized client to one or more unauthorized clients (step 162 in Fig. 6). The server analyzes which one of the N groups of authorized clients was sent the suspect key. The identified group includes the compromised client, while the rest of the N groups of clients are eliminated. The process is then repeated for the identified group for the next i^{th} block in the data transmission (step 164 in Fig. 6).

Fig. 7 shows an example of this method in which a data transmission 170 is destined to 10,000 authorized clients, one of which is believed to be compromised. The data transmission 170 is segmented into four equal-size blocks 1-4 (i.e., M= 4). For the first block 1, the key generator generates ten different authorization keys (i.e., N=10) and assigns them to ten different groups of clients, with each group having 1,000 clients. One key is found to be illicitly transferred and the suspect group is identified. This first iteration thus narrows the population of potential traitors to 1,000.

For the second block 2, the key generator produces ten new authorization keys and assigns them to ten groups of 100 clients within the population. Again, one of the ten keys is found to be illegally conveyed and the suspect group is noted. The second iteration narrows the population of potential traitors to 100.

For the third block 3, the key generator produces ten new authorization keys and assigns them to ten groups of 10 clients within the reduced population. The third iteration narrows the population of potential traitors to 10.

Finally, for the fourth block 4, the key generator produces ten new authorization keys and assigns each one to one client in the suspect population. When one of these keys is transferred illegally, the operator can pinpoint the compromised client and initiate legal proceedings against that user.

Accordingly, by properly selecting the number of segments M and the number of keys N for each segment, the operator can precisely identify the compromised client during a single data transmission.

The implementation described above employs a security device based on cryptographic functions. This invention may also be utilized in connection with security devices that employ other types of encoding/decoding technologies. For instance, rather than authorization keys, the authorized clients might be given authorization passwords or numbers for use in receiving broadcast content. As another alternative, the authorized client might be supplied with descrambling codes, or the like, to enable receipt of a scrambled data transmission.

The invention has been described in language more or less specific as to structural and methodical features. It is to be understood, however, that the invention is not limited to the specific features described, since the means herein disclosed comprise preferred forms of putting the invention into effect. The invention is, therefore, claimed in any of its forms or modifications within the proper scope of the appended claims appropriately interpreted in accordance with the doctrine of equivalents.

CLAIMS

1. A method for discovering an identity of an authorized security device that is illicitly transferring decoding capabilities for use in unauthorized security devices, comprising the following steps:

supplying different decoding capabilities to different authorized security devices, the decoding capabilities being used to decoded data that is delivered in an encoded format; and

in an event that one of the different decoding capabilities is illicitly transferred to an unauthorized security device, analyzing which one or more authorized security devices received said one decoding capabilities to identify a reduced set of one or more authorized security devices which includes the compromised security device.

2. A method as recited in claim 1, further comprising the step of repeating the supplying and analyzing steps to systematically eliminate non-compromised security devices from said reduced set until the compromised security device is identified.

3. A method as recited in claim 1, wherein:

the supplying step comprises the step of supplying a different decoding capabilities to each one of the authorized security devices; and

the analyzing step comprises the step of identifying which one of the authorized security devices was supplied with the illicitly transferred decoding capabilities.

4. A computer-readable medium having computer-executable instructions for performing the steps of the method as recited in claim 1.

5. A computing system programmed to perform the steps of the method as recited in claim 1.

6. A method for discovering an identity of an authorized security device that is illicitly transferring cryptographic keying material for use in unauthorized security devices, comprising the following steps:

supplying a first keying material to a first group of authorized security devices in a population of the authorized security devices;

supplying a second keying material to a second group of authorized security devices in the population; and

in an event that one of the first or second keying material is illicitly transferred to a unauthorized security device, identifying the corresponding first or second group of authorized security devices as including the compromised security device.

7. A method as recited in claim 6, further comprising the step of, in an event that the first keying material is illicitly transferred, repeating the supplying and identifying steps using the first group of authorized security devices as the population.

8. A method as recited in claim 6, further comprising the step of, in an event that the second keying material is illicitly transferred, repeating the supplying and identifying steps using the second group of authorized security devices as the population.

9. A computer-readable medium having computer-executable instructions for performing the steps of the method as recited in claim 6.

10. A computing system programmed to perform the steps of the method as recited in claim 6.

11. A method for discovering an identity of an authorized security device that is illicitly transferring cryptographic keying material for use in unauthorized security devices, comprising the following steps:

(a) segmenting a data transmission destined to the authorized security devices into M blocks;

(b) for an i^{th} block of the M blocks, supplying N different keying materials to N groups of authorized security devices to enable the security devices to receive the i^{th} block of the data transmission;

(c) in an event that one of the N keying materials is determined to be illicitly transferring from an authorized client to an unauthorized client, analyzing which of the N groups of authorized security devices received said one keying material being illicitly transferred to identify that group as including the compromised security device; and

(d) repeating steps (b) and (c) for each i^{th} block of the transmission, where i = 1 to M.

12. A method as recited in claim 11, wherein the variables M and N are selected to enable identification of the compromised security device during said data transmission.

13. A computer-readable medium having computer-executable instructions for performing the steps of the method as recited in claim 11.

14. A computing system programmed to perform the steps of the method as recited in claim 11.

15. In a system for distributing encrypted content to multiple authorized users, a method for discovering an identity of an authorized security device that is known to be compromised as illicitly transferring cryptographic keying material to unauthorized security devices, comprising the following steps:

distributing different authorization keys to different authorized security devices;

delivering one or more session keys to the authorized security devices, the security devices using the authorization keys to decrypt the sessions keys and using the session keys to decrypt the content;

tracing which one of the different authorization keys is illicitly transferred to an unauthorized security device; and

identifying a reduced set of one or more authorized security devices as possible security devices that illicitly transferred the authorization keys, the reduced set including the compromised security device.

16. A method as recited in claim 15, further comprising the step of repeating the steps of distributing, delivering, tracing, and identifying for the reduced set of authorized security devices.

17. A method as recited in claim 15, wherein:

the distributing step comprises the step of distributing different authorization keys to groups of security devices;

the identifying step comprises the step of identifying one of the groups as including the compromised security device; and

further comprising the step of repeating the steps of distributing, delivering, tracing, and identifying for each identified group of authorized security devices until the compromised security device is discovered.

18. A method as recited in claim 15, wherein the distributing step comprises distributing a different authorization key to each of the authorized security devices, and the identifying step comprises identifying one authorized security device as the compromised security device.

19. In a data delivery system for sending encrypted data from a server to multiple authorized clients, the server and the clients each having a computer-readable medium, the computer-readable media on the server and the clients having computer-executable instructions for performing steps comprising:

supplying different keying material from the server to different authorized clients;

utilizing the keying material at the authorized clients to decrypt the data served from the server; and

in an event that one of the different keying materials is determined to be illicitly transferred from an authorized client to an unauthorized client, analyzing at the server which one or more authorized clients was sent said one keying material to identify a reduced set of one or more authorized clients which includes the compromised client.

20. Computer-readable media as recited in claim 19, further comprising computer-executable instructions for performing the following steps:

sending the encrypted data to the authorized clients in blocks; and

supplying a new set of different keying materials for each block.

21. In a data delivery system for supplying encrypted data from a server to multiple authorized clients, a traitor detection system for discovering authorized clients that have illicitly transferred decryption capabilities to unauthorized clients, comprising:

a key generator located at the server, the key generator producing different keying material for use in decrypting the encrypted data;

a key-client associator located at the server to associate the different keying material with different authorized clients;

a data decryptor located at each of the authorized clients to decrypt the encrypted data supplied from the server using one of the keying materials; and

in an event that one of the different keying materials is determined to be illicitly transferred from an authorized client to an unauthorized client, the key-client associator evaluating which of the authorized clients was sent said one keying material to identify one or more of the authorized clients as a possible source of the illicit transfer.

22. A traitor detection system as recited in claim 21, wherein the key generator produces keying material for each one of the authorized clients to enable precise identification of the authorized client that made the illicit transfer.

23. In a data delivery system for supplying encrypted data to multiple authorized clients, a computer-readable medium having computer-executable instructions for performing the following steps:

generating different keying materials for use in decrypting the encrypted data;

creating a key-client association file which relates the keying materials to different authorized clients, the keying material being made available to the authorized clients for use in decrypting the data; and

in an event that one of the different keying materials is determined to be illicitly transferred from an authorized client to a unauthorized client, identifying from the key-

client association file one or more of the authorized clients that were supplied with said illicitly transferred keying material as a possible source of the illicit transfer.

24. A computer-readable medium as recited in claim 23, further comprising computer-executable instructions for performing the following steps:

delivering the encrypted data to the authorized clients in blocks; and

generating a new set of different keying materials for each block.

25. A computer-readable medium as recited in claim 23, further comprising computer-executable instructions for performing the step of generating a different keying material for each one of the authorized clients.

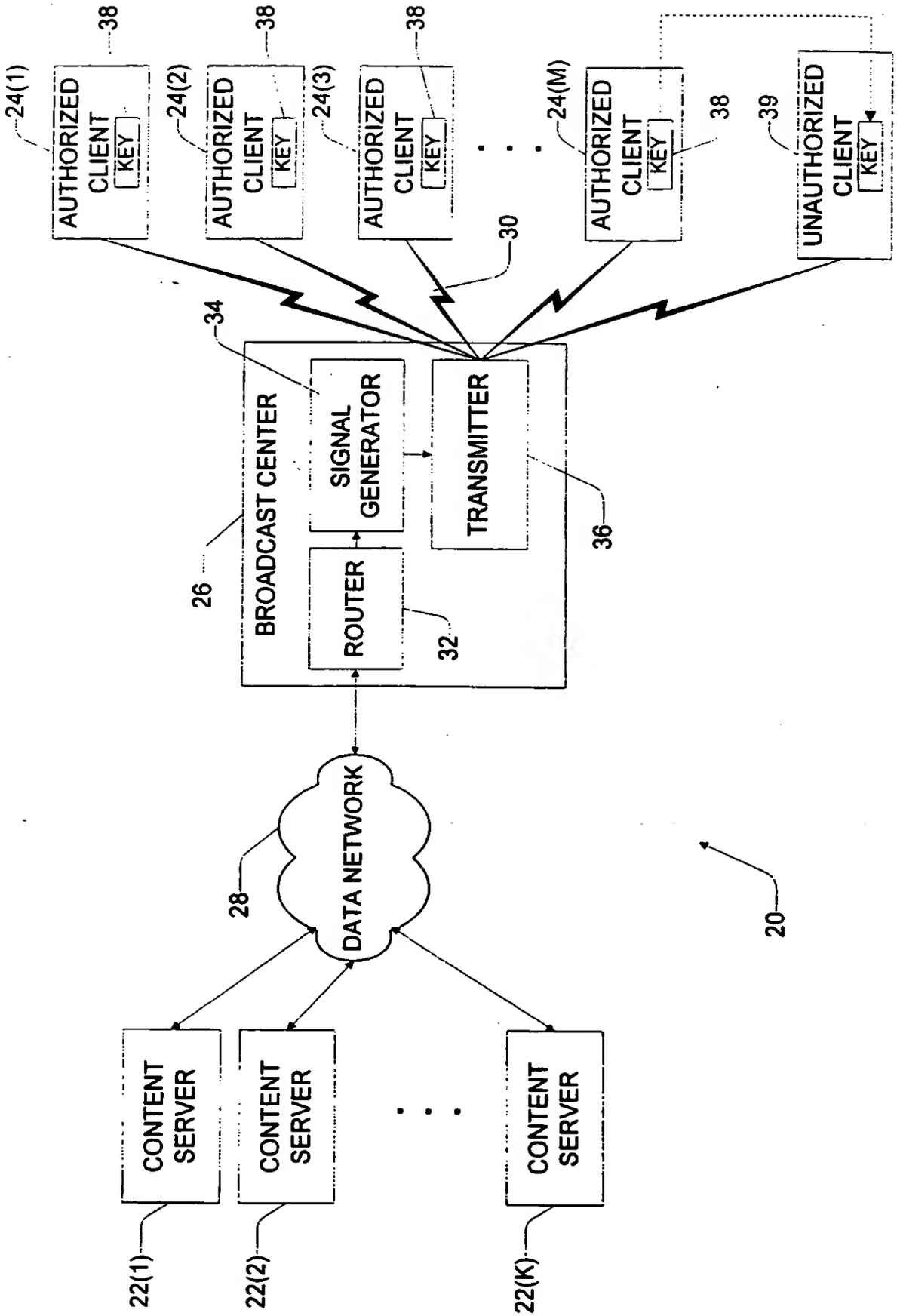

24(1)
AUTHORIZED CLIENT
KEY
38
24(2)
AUTHORIZED CLIENT
KEY
38
24(3)
AUTHORIZED CLIENT
KEY
38
24(M)
AUTHORIZED CLIENT
KEY
38
39
UNAUTHORIZED CLIENT
KEY
30
34
BROADCAST CENTER
SIGNAL GENERATOR
TRANSMITTER
ROUTER
26
32
36
DATA NETWORK
28
20
CONTENT SERVER
CONTENT SERVER
CONTENT SERVER
22(1)
22(2)
22(K)

Fig. 1

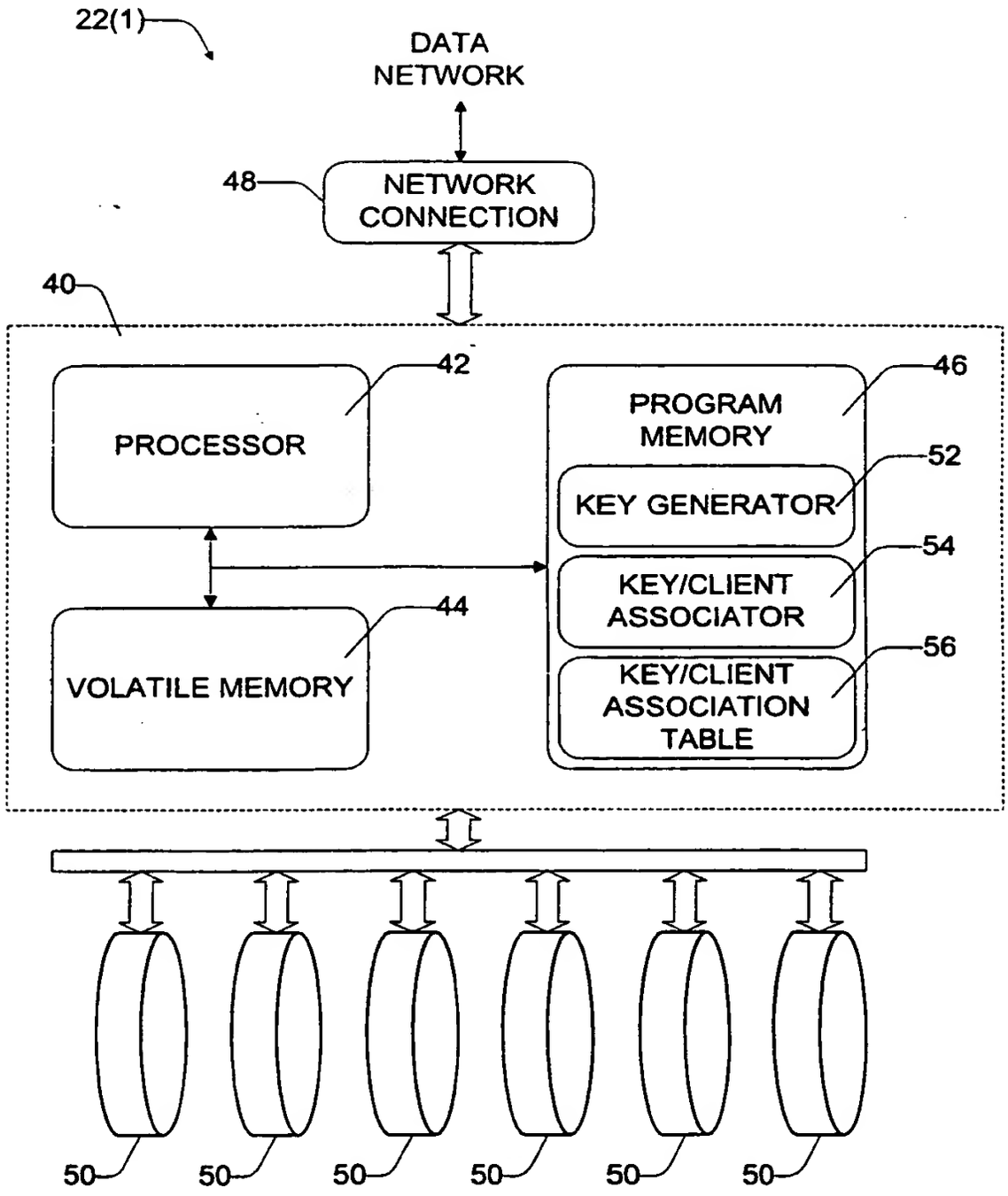

22(1)
DATA NETWORK
48
NETWORK CONNECTION
40
42
PROCESSOR
46
PROGRAM MEMORY
52
KEY GENERATOR
54
KEY/CLIENT ASSOCIATOR
56
KEY/CLIENT ASSOCIATION TABLE
44
VOLATILE MEMORY
50
50
50
50
50
50

Fig. 2

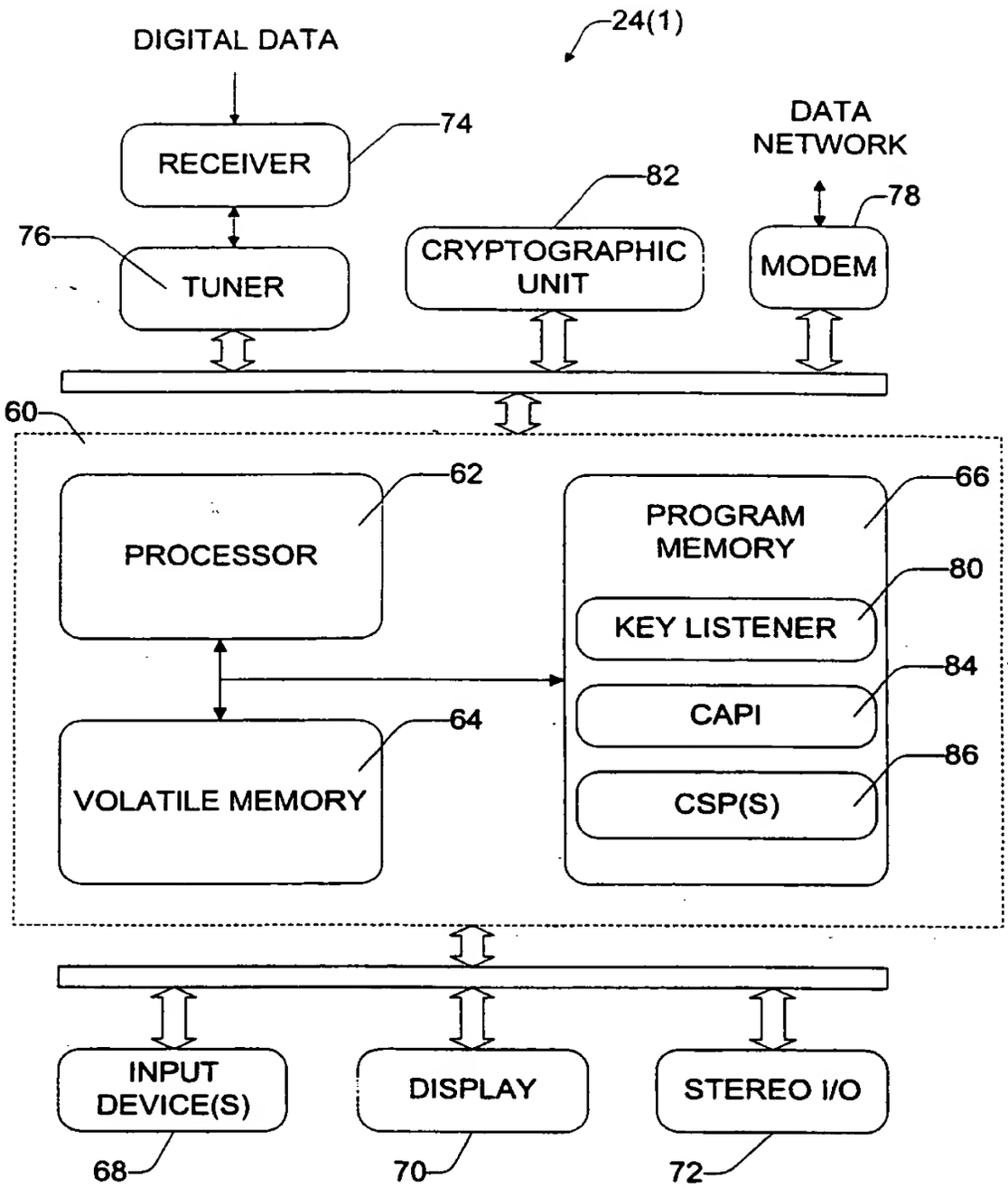


Fig. 3

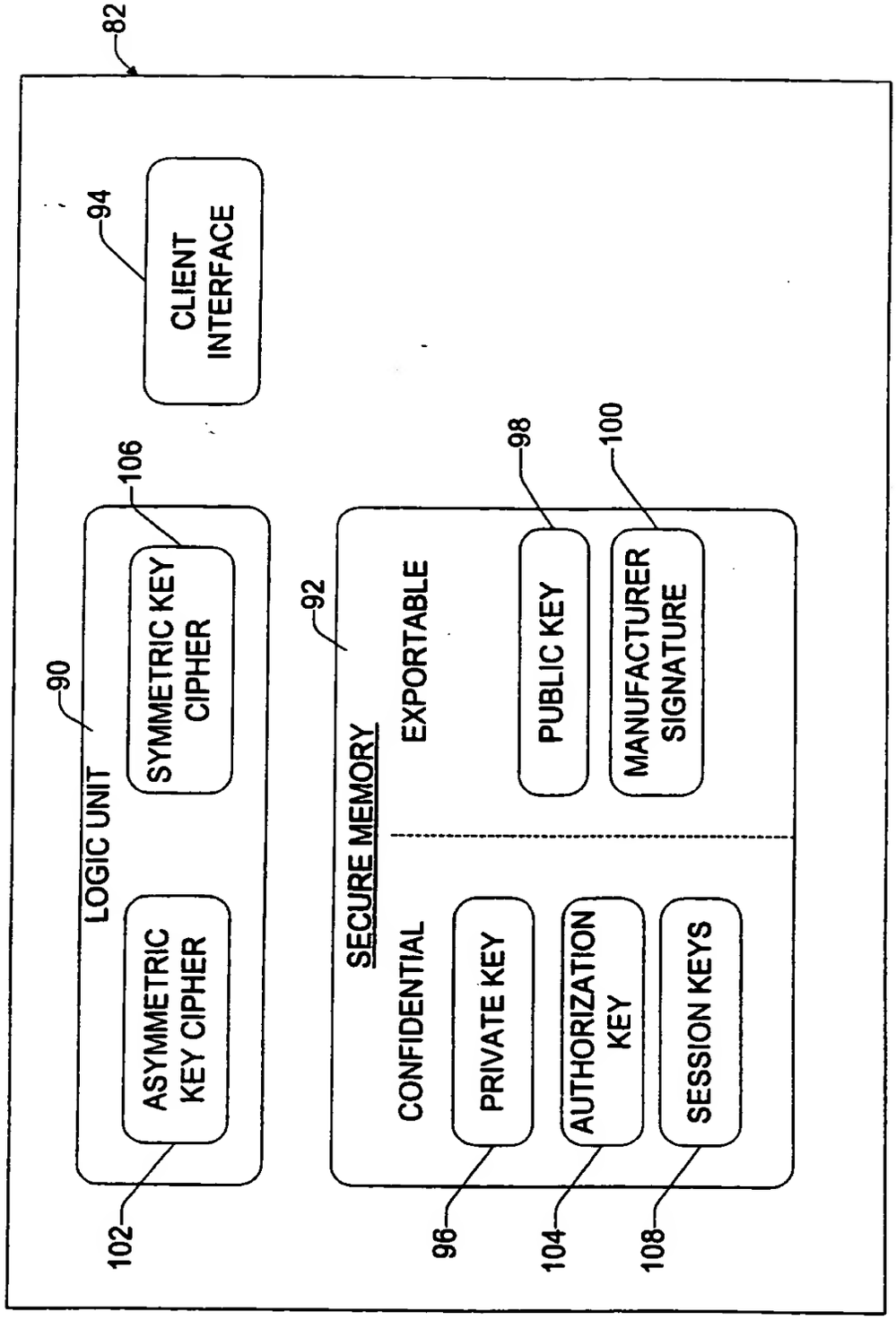

82
94
CLIENT INTERFACE
106
SYMMETRIC KEY CIPHER
90
LOGIC UNIT
ASYMMETRIC KEY CIPHER
102
92
SECURE MEMORY
EXPORTABLE
98
PUBLIC KEY
100
MANUFACTURER SIGNATURE
CONFIDENTIAL
PRIVATE KEY
AUTHORIZATION KEY
SESSION KEYS
96
104
108

Fig. 4

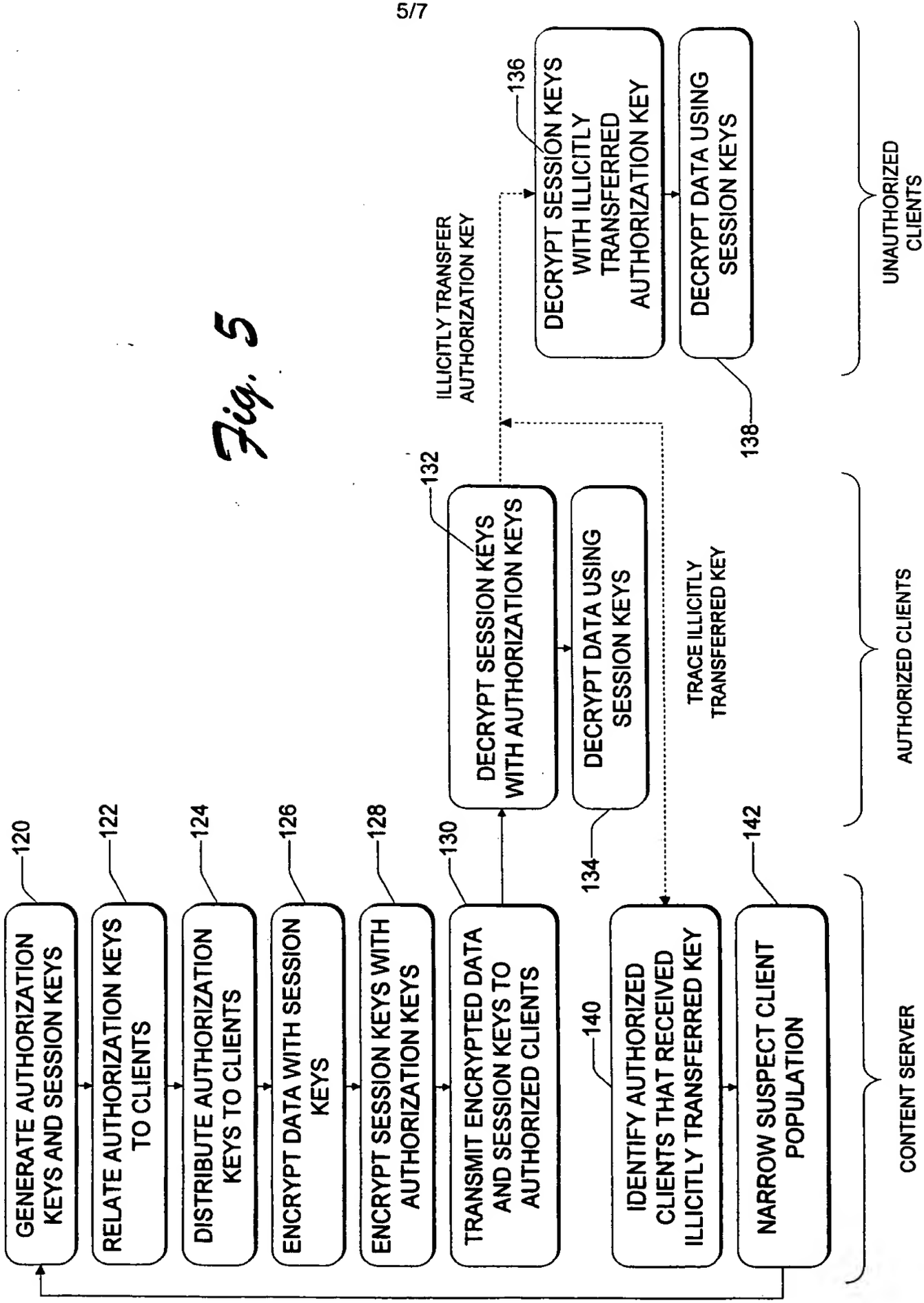


Fig. 5

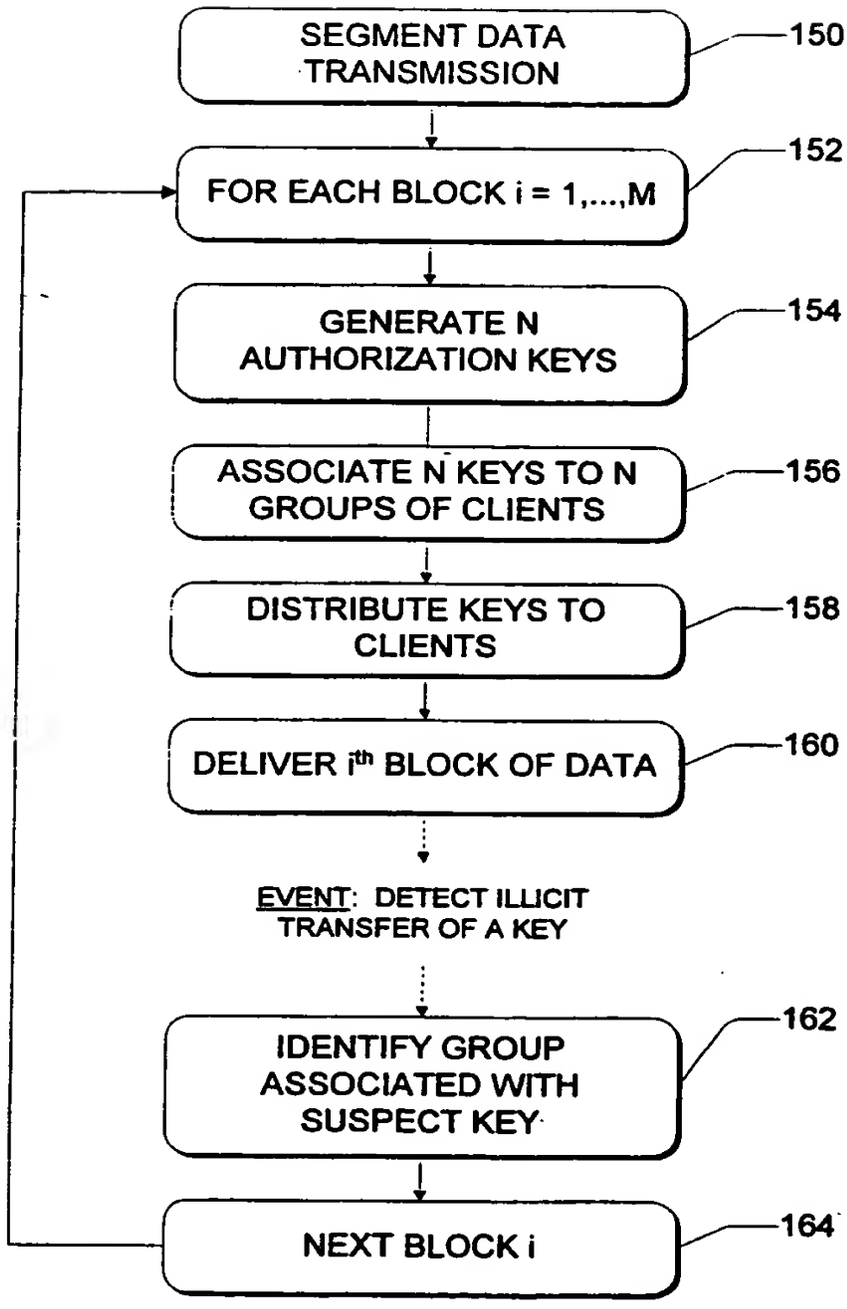

SEGMENT DATA TRANSMISSION
150
FOR EACH BLOCK i = 1,...,M
152
GENERATE N AUTHORIZATION KEYS
154
ASSOCIATE N KEYS TO N GROUPS OF CLIENTS
156
DISTRIBUTE KEYS TO CLIENTS
158
DELIVER ith BLOCK OF DATA
160
EVENT: DETECT ILLICIT TRANSFER OF A KEY
IDENTIFY GROUP ASSOCIATED WITH SUSPECT KEY
162
NEXT BLOCK i
164

Fig. 6

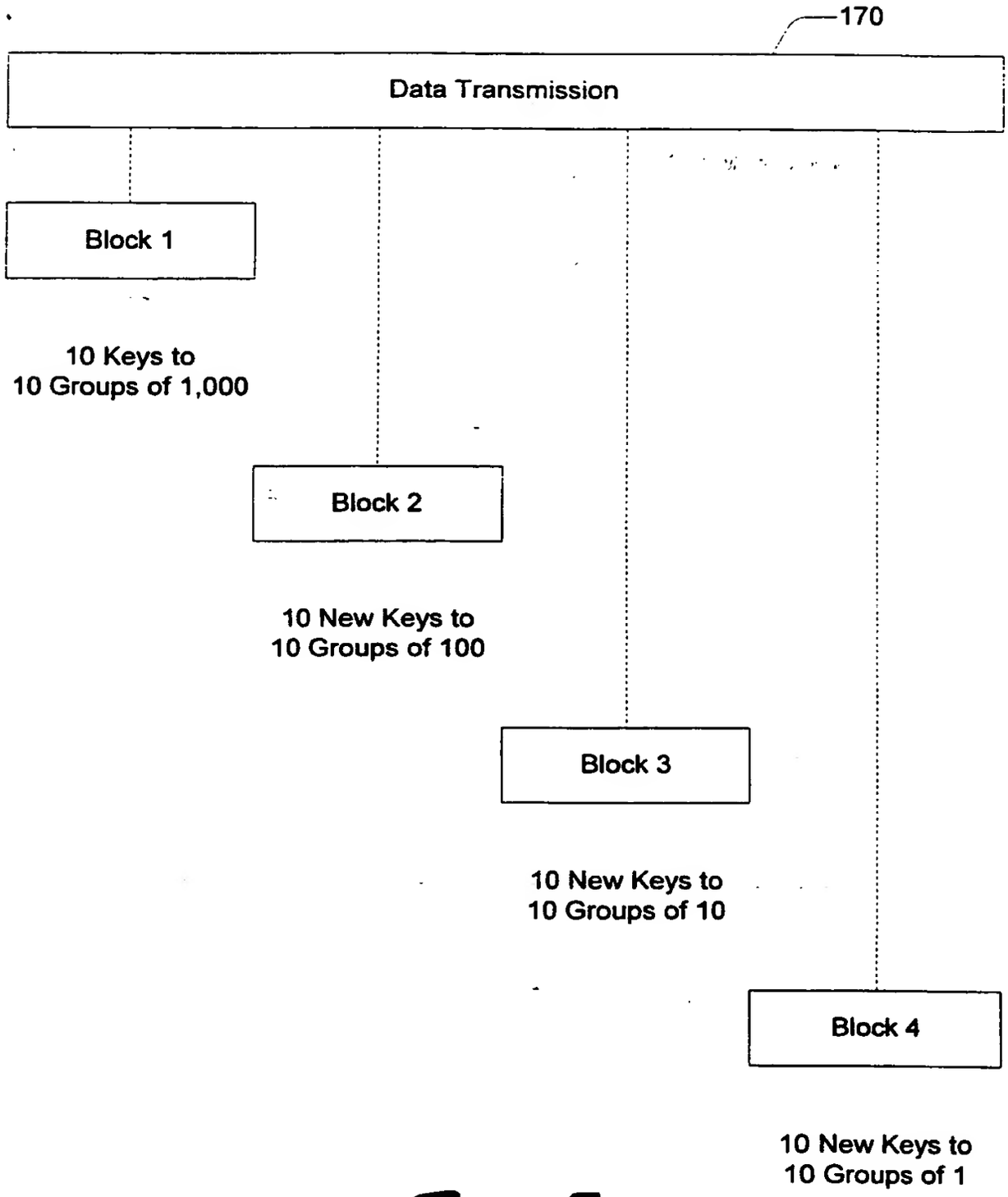


Fig. 7

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 9/08

A3

(11) International Publication Number: WO 99/19822

(43) International Publication Date: 22 April 1999 (22.04.99)

(21) International Application Number: PCT/US98/19352

(22) International Filing Date: 16 September 1998 (16.09.98)

(30) Priority Data:
08/949,438 14 October 1997 (14.10.97) US

(71) Applicant: MICROSOFT CORPORATION [US/US]; One Microsoft Way, Redmond, WA 98052-6399 (US).

(72) Inventors: BIRDWELL, Kenneth, J.; 17452 N.E. 12th Street, Bellevue, WA 98008-3816 (US). YACOBI, Yacov; 5050 W. Mercer Way, Mercer Island, WA 98040 (US).

(74) Agents: LEE, Lewis, C. et al.; Suite 430, W. 201 North River Drive, Spokane, WA 99201 (US).

(81) Designated States: JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

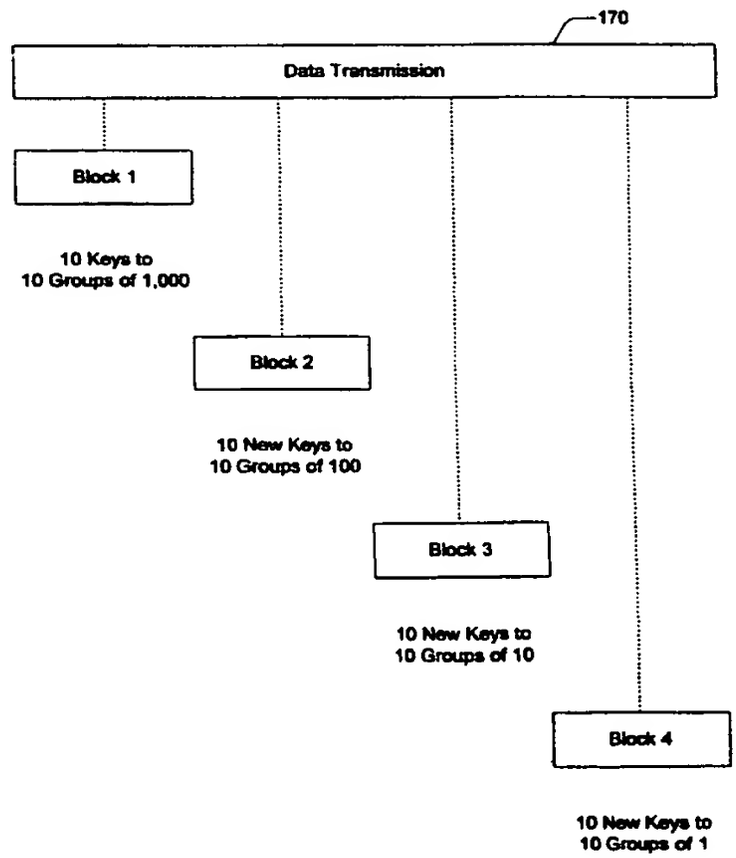
Published
With international search report.

(88) Date of publication of the international search report:
17 June 1999 (17.06.99)

(54) Title: SYSTEM AND METHOD FOR DISCOVERING COMPROMISED SECURITY DEVICES

(57) Abstract

A data delivery system has a content server or other mechanism for delivering encoded content to multiple authorized clients. The authorized clients are equipped with security devices having decoding capabilities to decode the content. Unauthorized clients are prevented from decoding the content because they are not supplied with the decoding capabilities. As part of the data delivery system, a traitor detection system is provided to discover an identity of an authorized client that has been compromised and is illicitly transferring decoding capabilities to unauthorized clients. The traitor detection system generates different decoding capabilities and creates an association file which relates the different decoding capabilities to different authorized clients. The decoding capabilities are traced to determine which of them is illicitly transferred to an illegitimate user. In the event that one of the decoding capabilities is illicitly transferred, the traitor detection system consults the association file to identify one or more of the authorized clients that were originally supplied with the illicitly transferred decoding capabilities. The identified set of clients includes the compromised client. The process is repeated for the identified set of clients with a new set of decoding capabilities to successively narrow the field of possible pirating clients, until the compromised security device is precisely pinpointed.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

INTERNATIONAL SEARCH REPORT

Inter. onal Application No
PCT/US 98/19352

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CHOR B ET AL: "Tracing traitors" ADVANCES IN CRYPTOLOGY - CRYPTO '94. 14TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS, ADVANCES IN CRYPTOLOGY - CRYPTO '94. 14TH INTERNATIONAL CRYPTOLOGY CONFERENCE PROCEEDINGS, SANTA BARBARA, CA, USA, 21-25 AUG. 1994, pages 257-270, XP002097845 ISBN 3-540-58333-5, 1994, Berlin, Germany, Springer-Verlag, Germany	1,15,19, 21
A	see page 259, last paragraph - page 260, last line see page 263, line 9 - line 20 see page 266, line 1 - page 267, line 12	6,11

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 April 1999	15/04/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)